SPECIFICATION

Electronic Version 1.2.8

Stylesheet Version 1.0

POSITION PRIVACY IN AN ELECTRONIC DEVICE

Cross Reference to Related Applications

This application is a continuation of U.S. Patent Application No. 09/690,001 filed October 16, 2000.

Background of Invention

[0001] The present invention defines a system for enhancing a privacy in enhancement in an electronic device with automatic position location detection.

[0002] Modern electronic devices often include automatic position location detection technology. For example, the modern cellular phone may include a satellite positioning system such as a GPS device. Other cellular phones, referred to as a WAP phones, also automatically keep track of the users position.

[0003] Figure 1 shows an electronic device, which can be a wap phone, regular cellular phone, or any other electronic device 100. The device is shown with electronic circuitry including electronic processor 110 which processes signals from both GPS device 115, and from a codec 120. The processor also controls an RF device 125.

[0004] The electronic device automatically determines its position. In this embodiment, it does so by communicating with a constellation of global position detecting satellites 130, for automatic determination of position. The electronic device may also communicate with the server 140, such as to a base station. The electronic device may communicate its determined position to the server. This may be done, for example, for emergency purposes. In the case of a WAP device, this may be done simply to monitor the position of the cellular phone. The server may output the position, shown as 150.

Summary of Invention

[0005] The present application defines a device which enhances privacy in such a system. Specifically, the present application teaches a device which selectively prevents the electronic device from transmitting its position. This hence allows selection of an enhanced privacy mode.

Brief Description of Drawings

[0006] These and other aspects of the invention will be described in detail with reference to the accompanying drawings, wherein:

[0007] Figure 1 shows are block diagram of an electronic device with a built-in automatic position location detection system;

[0008] Figure 2 shows a first embodiment of a privacy enhancing device for an electronic element;

[0009] Figures 3A and 3B show a passive version of the privacy enhancing device using an RF blocking technique; and

[0010] Figure 4 shows an active jammer device which actively produces a signal to prevent the reporting of position.

Detailed Description

[0011] The first embodiment is shown in Figure 2. In this embodiment, the electronic device is a portable telephone such as a cellular phone. However, it should be understood that other electronic devices, such as computers, personal digital assistants, or any other device which is capable of communicating in any way, may use similar techniques to those disclosed herein. A portable phone 200 has a normal user interface 205, and other structure such as display, etc. The device also includes a positioning device 210. In this embodiment, a position detection block control 220 is provided. This is an actuation mechanism, such as a button which can be pressed to deactivate the function of the positioning device 210. The unit"s normal position forms an enable signal 225 which enables the position detector 210, allowing the position detector to determine its position, and report that position to a remote source, such as a base station. When the button is in its override position, an indicator

225 is illuminated, indicating the privacy mode has been entered. In this privacy-enhanced state, the enable signal is removed, thereby preventing position detector 210 from reporting its position.

[0012] A concern, however, is that some users, either hackers or others with more aura of authority, may use this system in a way which determines position surreptitiously, e.g., even when the button is placed on override. For example, law-enforcement officials might use this system to keep track of someone without their knowledge. One way to do this might be to fake an emergency call or the like. Doing this, however, may have serious privacy implications.

[0013] If a manufacturer includes a back door into the system, that back door might be used to determine the position of a person, without their authority or knowledge.

[0014] A test module 250 can be used to test the degree of privacy associated with the electronic device. This test module is connectable to the server 260. It also runs a software layer 255 which can be updated via channel 270, e.g., over the Internet. The test module 250, in operation, communicates with a service over the internet. The service employs experts to research and store the latest and most up-to-date way of improperly obtaining position in such a system. This is available via update 270 from the Internet. This may be carried out as a subscription service, in a similar way to the operations currently done to update virus definitions. The Internet returns ways of hacking the position detection prevention, which can hence be used by the test module to evaluate the privacy provided by the actuation 220.

[0015] The test module sends a request for position location to the phone 200, using the best available techniques. The phone returns information, and this information is evaluated by the server 260. Server 260 returns an evaluation of the operation to the test module 250. This can provide a user with an indication of the level of privacy they have obtained.

[0016]

Another embodiment is shown in Figures 3A and 3B. This embodiment may be most usable with a satellite positioning system in a telephone. In this kind of phone, both sets of electronics -- the GPS and the codec -- may use a common processor. However, a GPS system often requires a separate antenna shown as 300. The separate

antenna may be very sensitive to reception. For example, while cellular telephones can often be used indoors, corresponding GPS devices may not be usable in the same situations. Moreover, each separate telephone type will have a GPS antenna 300 placed in a specified location. There are relatively few telephone types in common use, usually less than 50 types. This system finds, for each telephone type, where the GPS antenna will be placed. The device 350 is made of an RF absorbing or reflecting material such as metal. The device is also made in way which allows it to be temporarily attached to the telephone, e.g., by clipping on to the phone. For example, the device may fit on both sides of the telephone 310 and 320 and wrap around the telephone to cover areas adjacent the antenna on both of the surfaces. The cover 350 covers both sides of the antenna 300, and therefore prevents GPS operation while the cover is clamped into place. In this way, privacy can be effectively temporarily enhanced. Figures 3A and 3B show two different places where the shield could be attached; but it should be understood that the shield could be attached in many different places.

[0017] One of the stated uses of GPS in a portable phone is for use in an emergency. When the user dials 911, the GPS device allows the emergency authorities to determine the user"s precise location. In order to allow this, the cover can be maintained in place during all operations other than emergencies. During emergencies, the cover can be removed. But once the cover is removed, the position of the electronic device can be automatically detected, as usual.

[0018] The system of figures 3A and 3B may not work with certain phones. An alternative system is shown in figure 4. In this phone, an active jammer module 400 is provided. The jammer module either supplants or fools the system into obtaining false position information. For example, the jammer module may provide false satellite information, e.g., indicating a false satellite position.

[0019]

Satellite positioning system information is often provided in broad spectrum noise. The jammer 400 may produce broad spectrum noise, which includes information indicative of three satellites, but which is transmitted at a sufficiently low power to be receivable only at a very short range. In the system of figure 4, the jammer can also be attached using attachment clips 404. The attachment can place

the transmitter of the jammer in close proximity with the satellite positioning system antenna.

[0020] The jammer information can produce outputs that indicate a false location, for example. Similar operations can be carried out with WAP phones. In a WAP phone, for example, the system may override the carrier, or tell the carrier false information about where the phone is located. This may include providing false triangulation information into the system or the like.

[0021] Other modifications are possible and are within the disclosed invention.